CLAIMS

1. In an electronic communications system for providing communication between at least a first party and a second party and having means for connecting said first and second parties for electronic communication, and means for controlling secure communication between said first and second parties by the exchange of security codes between said parties,

a method of controlling a plurality of separate electronic communications between said first and second parties, said method comprising the steps of :

(a) initially securely exchanging a seed value between said first and second parties;

(b) exchanging a mathematical advance function between said parties; and

(c) exchanging a one-way hash function between said parties;

said method further comprising, prior to each separate communication, the steps of :

(d) applying said advance function to the seed value to create a new seed value at each of said parties;

(e) applying said hash function to said new seed value to create a said security code at each of said parties;

(f) communicating said security code generated at said first party to said second party;

(g) comparing said communicated security code with said security code generated at said second party; and

(h) if said security codes are the same at both parties, permitting the respective communication to take place between said first and second parties.

2. A method as claimed in claim 1 wherein said separate communications each follow a disconnection of said first and second parties , said steps (a) to (c) preceding such disconnection, said method including the further step of physically re-establishing said connection between said parties prior to said steps (d) to (g).

3. A method as claimed in claim 1 wherein said advance function is non-recursive.

4. A method as claimed in claim 3 wherein said advance function is an arithmetic function.

5. A method as claimed in claim 1 wherein said advance function and said hash function are also exchanged securely.

6. A method as claimed in claim 1 in which, if said security code is the same, after said comparing step (g), comprises the further steps, prior to permitting resumption of communication between said first and second parties, of:

applying the advance function to said new seed value at each of said parties to create a further new seed value;

applying the hash function to said further new seed value to create a further security code at each of said parties;

communicating said further security code generated at said second party to said first party;

comparing said further security codes received at said first party with the further security code generated at said first party; and

if said further security code is also the same at both nodes, permitting said communication between said first and second parties to take place.

7. A secure electronic communications system comprising means for connecting at least a first party and a second party for electronic communication; and

means for controlling a plurality of separate electronic communications between said first and second parties by the exchange of security codes between said parties;

wherein said means for controlling includes:-

means for initially securely exchanging a seed value between said first and second parties;

means for exchanging a mathematical advance function between said parties; and

means for exchanging a one-way hash function between said parties;

means for applying said advance function to said seed value to create a new seed value at each of said parties prior to each separate communication;

means for applying said hash function to said new seed value to create a said security code at each of said parties;

means for communicating said security code generated at said first party to said second party;

means for comparing said communicated security code with said security code generated at said second party; and

means responsive to said security codes being the same at both parties to permit the respective communication to take place between said first and second parties.

8. A system as claimed in claim 7 wherein said separate communications each follow a disconnection of said first and second parties, said system including means for physically re-establishing said connection between said parties.

9. A system as claimed in claim 7 wherein said advance function is non-recursive.

10. A system as claimed in claim 9 wherein said advance function is an arithmetic function.

11. A system as claimed in claim 7 including said means for exchanging said advance function and said hash function securely.

12. A computer program, recorded on a medium, for use in an electronic communications system for providing communication between at least a first party and a second party, said system having means for connecting said first and second parties for electronic communication and means for controlling secure communication between said first and second parties by the exchange of security codes between said parties, said computer program comprising instructions which, when executed on a computer, carry out a method of controlling a plurality of separate electronic communications between said first and second parties, comprising the steps of :

(a) initially securely exchanging a seed value between said first and second parties;

(b) exchanging a mathematical advance function between said parties; and

(c) exchanging a one-way hash function between said parties;

said method further comprising, prior to each separate communication, the steps of :

(d) applying said advance function to the seed value to create a new seed value at each of said parties;

(e) applying said hash function to said new seed value to create a said security code at each of said parties;

(f) communicating said security code generated at said first party to said second party;

(g) comparing said communicated security code with said security code generated at said second party; and

(h) if said security codes are the same at both parties, permitting the respective communication to take place between said first and second parties.

13. A computer program as claimed in claim 12 wherein said separate communications each follow a disconnection of said first and second parties , said method steps (a) to (c) preceding such disconnection, said method including the further step of physically re-establishing said connection between said parties prior to said steps (d) to (g).

14. A computer program as claimed in claim 12 wherein said advance function is non-recursive.

15. A computer program as claimed in claim 14 wherein said advance function is an arithmetic function.

16. A computer program as claimed in claim 12 wherein said advance function and said hash function are also exchanged securely.

17. A computer program as claimed in claim 12 in which, if said security code is the same, after said comparing step (g), carries out the further method steps, prior to permitting resumption of communication between said first and second parties, of:

applying the advance function to said new seed value at each of said parties to create a further new seed value;

applying the hash function to said further new seed value to create a further security code at each of said parties;

communicating said further security code generated at said second party to said first party;

comparing said further security codes received at said first party with the further security code generated at said first party; and

if said further security codes are also the same at both parties, permitting said communication between said first and second parties to take place.

18. A client computer connectable for secure communication with a server computer, said client computer comprising:

means for receiving from said server computer a seed value, a mathematical advance function and a one-way has function;

means for applying said advance function to said seed value to create a new seed value;

means for applying said hash function to said new seed value to create a security code;

and means for communicating said security code to said server computer;

whereby said server computer permits secure communication with said client computer if a security code correspondingly calculated by said server is identical to said security code communicated by said client computer.

19. A client computer as claimed in claim 18 wherein said advance function is non-recursive.

20. A client computer as claimed in claim 19 wherein said advance function is an arithmetic function.

21. A client computer as claimed in claim 18 which is a cellular telephone.

22. A client computer as claimed in claim 21 which is WAP enabled.

23. A client computer as claimed in claim 18 which is a personal digital assistant.

24. A server computer connectable for secure communication with one or more client computers, said server computer comprising means for providing to said client computer a seed value, a mathematical advance function and a one-way hash function;

means for applying said advance function to said seed value to create a new seed value;

means for applying said hash function to said new seed value to create a security code;

means for receiving a correspondingly calculated security code from said client computer;

means for comparing said security codes; and

means responsive to said security codes being the same to enable secure communication to take place with said client computer.

25. A server computer as claimed in claim 24 wherein said advance function is non-recursive.

26. A server computer as claimed in claim 25 wherein said advance function is an arithmetic function.